Emerging IEEE 802.11 Standards

Luke Qian

As the popularity of IEEE 802.11 wireless LANs (WLANs) grows rapidly, many new 802.11 wireless standards are emerging. New 802.11 standards are being developed in two major categories: specifications that make use of advanced wireless technologies in Radio Frequency (RF) and Physical layer (PHY), such as 802.11n, and specifications that address the needs in wireless network management, performance measurements, inter-networking, fast roaming, and the needs in other various specific applications and use scenarios. These include 802.11k, 802.11p, 802.11r, 802.11s, 802.11T, 802.11u, 802.11v, 802.11w and 802.11y. In this chapter, we discuss briefly the goals and scopes of these emerging standards. Emphasis will be given on 802.11n standard because of the significance in the technology advances it brings in.

1. IEEE 802.11n: Enhancements for Higher Throughput

802.11n is a long anticipated upgrade to the IEEE 802.11a/b/g wireless local-area network standards. It is expected to bring significant increase in MAC throughput of over 100 megabits per second (Mbps) and an enhanced communication range in the 2.4 and 5 GHz bands. 802.11n is also required to make efficient use of the unlicensed spectral resources by achieving at least 3 bits per second per Hz at the highest 802.11n rate.

The first draft of 802.11n supports PHY rates as high as 270 Mbps or five times that of a 802.11a/g network, which runs at 54 Mbps. The PHY rates can increase even more, up to 600 Mbps with four spatial streams and 40 MHz bandwidth, in the longer term when more receiver and transmitter antennas are employed. Currently, many chip vendors have already shipped pre-11n devices and have delivered the performance enhancements in both higher throughput and longer range promised by 802.11n.

High throughput (HT) devices are compliant with 802.11a/b/g standards. 802.11n defines a number of modes for backwards compatibility and interoperability with 802.11a and/or 802.11g.

802.11n builds upon existing 802.11 standards with enhancements to the MAC and the use of multiple-input multiple-output (MIMO) technologies. MIMO employs multiple transmitter and receiver antennas to allow for simultaneous data streams. The technology is

\[a \text{ Cisco Systems, Inc}\]
Emerging IEEE 802.11 Standards

capable of increasing data throughput via spatial multiplexing and increasing range via spatial diversity.

1.1.1 802.11n PHY

802.11n PHY is a high throughput orthogonal frequency division multiplexing (HT OFDM) system operating in the unlicensed 2.4 GHz and 5 GHz bands. The 802.11n PHY accommodates the required high throughput using MIMO, channel binding, beam forming, and Space-Time Block Coding (STBC). A number of other PHY features are also included in 802.11n to help meet the requirements.

The 802.11n PHY operates in one of three modes: Non-HT mode, Mixed mode, and the optional Green Field mode. In the Mixed mode, packets are transmitted with a preamble compatible with the non-HT receivers followed by a HT specific part for estimation of the MIMO channel. The Mixed mode enables non-HT devices to detect the transmission of a Mixed mode HT packet. In the Green Field mode, the non-HT compatible part of the Mixed mode preamble is omitted for higher efficiency. The two HT PLCP packet formats are illustrated in Figure 1.1.

![Figure 1.1: 802.11n PLCP Packet Formats.]

1.1.1.1 MIMO

802.11n employs a mandatory basic MIMO of space division multiplexing. With MIMO, multiple spatial streams transmitted at the same time significantly increase the data rate (Figure 1.2).

1.1.1.2 40 MHz Channel Binding

Optionally, 802.11n allows for two adjacent 20 MHz channels to be combined into a single 40 MHz channel. This enables twice the amount of data to be carried in a single OFDM symbol. One of the tradeoffs is that it will reduce the number of total available channels. Spectrum use may not be optimal when the interference between devices in the various channels is taken into account. This is especially a concern in the 2.4 GHz band where the available channels are less than in 5 GHz.

1.1.1.3 Beam Forming

Beam forming is an optional technique adopted in 802.11n in which the transmitter utilizes the knowledge of the MIMO channel to generate a spatial mapping matrix that will improve reception in the receiver. There are two flavors of beam forming: implicit beam forming and explicit beam forming.
Emerging IEEE 802.11 Standards

Implicit beam forming uses the fact that the channel between STA A and STA B is the transpose of the channel between STA B and STA A. In reality, the actual channel includes the transmit chain in STA A and receive chain in STA B. So a calibration procedure is needed to correct for the difference in the measured channel.

In explicit beam forming, a transmitting STA needs the receiving STA to measure and send the channel matrices or the mapping matrices. The matrices can be either uncompressed (which can be used directly by the transmitter) or compressed (which requires further processing by the transmitter).

1.1.1.4 STBC

Space-Time Block Coding (STBC) is an optional PHY feature in 802.11n. STBC transmits multiple copies of a data stream across multiple antennas. On the receiving side, STBC combines all the received copies of signals optimally. The various received versions of the data provides the redundancy that results in a higher probability for one or more of the received copies of the data to be correctly decoded.

1.1.1.5 Other 802.11n PHY Features

There are a number of other optional PHY features introduced in 802.11n to help achieve the high throughput and increased range. These include:

- Green Field (GF) mode: an optional HT mode which provides high efficiency by omitting the backward-compatible portion in the preambles of packets operating in the HT Mixed mode.
- Short guard interval (GI): use of a short guard interval of 400 ns rather than a regular long GI of 800 ns.
- Low density parity check (LDPC) codes: an advanced error correcting code introduced along with an iterative probability-based decoding algorithm developed by Gallager in the early 1960’s. Sparse random parity check matrices are used in constructing the codes.
4 Emerging IEEE 802.11 Standards

- Reduced Interframe Space (RIFS): Allows a transmitter to transmit a sequence of PPDUs each separated by 2 μs.

1.1.2 802.11n MAC

The major function of 802.11n MAC is to meet the high throughput requirement under the constraint of the 802.11e QoS specifications. It also provides legacy compatibility protection and interoperability. In addition, new frames (such as sounding frames for channel measurements) are introduced to support HT PHY capabilities.

1.1.2.1 High Throughput Support

802.11n introduces extra PHY overheads to accommodate the transmission of 802.11n frames with the advanced PHY technologies. The overheads, along with the shortened transmission time of the payload due to the higher data rates, greatly reduces the MAC efficiency. The following plot in Figure 1.3 shows the MAC efficiency for an example of a point-to-point setting at a PHY rate of 243Mbps. For a packet size within the range of regular frame sizes, the MAC efficiency is found to be well below 20%.

![Figure 1.3: MAC Efficiency versus Frame Size.](image)

To better understand the cause of this low MAC efficiency, Figure 1.4 breaks up the transmission time for an example of a frame and its acknowledgement. Apparently, channel access, inter-frame spacing, and PHY headers in particular, take up a considerable amount of the entire packet transmission time. As a result, the transmission time taken by the payload portion becomes very small.

Increasing the MAC efficiency to realize the high data rates provided by HT PHY therefore becomes one of the major objectives in the development of 802.11n MAC enhancements. Since the MAC efficiency increases with the frame size, the major technique to achieve HT throughput in the 802.11n MAC is to perform frame aggregations. These include aggregated MSDU (A-MSDU), aggregated MPDU (A-MPDU), and RIFS Bursting.
A-MSDU defines an efficient MAC frame format as illustrated in Figure 1.5. A-MSDU aggregates multiple MSDUs in a single MPDU. Each sub-frame in an A-MSDU consists of a sub-frame header followed by a MSDU and 0-3 bytes of padding. The maximum allowed A-MSDU size is extended to around 4 KBytes and an optional 8 KBytes for MAC efficiency improvement.

All sub-frames in an A-MSDU must be addressed to the same receiver address because they share one single MAC header. In the same light, all sub-frames in an A-MSDU must be of the same access category (AC). Since there is only one single FCS for an A-MSDU, error recovery can be expensive and an error in any of the sub-frames will require the re-transmission of all the sub-frames in the A-MSDU.

A-MPDU is another form of aggregation in 802.11n. A-MPDU aggregates multiple MPDUs in a single PPDU as shown in Figures 1.6 and 1.7. The maximum allowed A-MPDU size is extended to around 64 KBytes, much longer than that of A-MSDU.

A-MPDU is purely a MAC function. The PHY has no knowledge of the MPDU boundaries and treats the A-MPDU as if it were a regular MPDU. Each sub-frame in an A-MPDU has its own FCS. When an error occurs to a sub-frame, it is possible to continue parsing the rest of the PPDU and recover them with the A-MPDU delimiters and the unique A-MPDU signature pattern embedded in the delimiters. This error recovery mechanism in A-MPDU makes it less expensive than A-MSDU when an error in a sub-frame occurs. On the other hand, since there are multiple MAC frames in a single A-MPDU, the Block ACK (BA) to acknowledge multiple frames has to be involved to accommodate the A-MPDU and this
Emerging IEEE 802.11 Standards

adds significant complexity and buffer requirement in the implementation of the A-MPDU. To offset the overheads relating to the use of BA, a number of BA enhancements are introduced in the 802.11n MAC. For example, it allows implicit BA without a BA request and a compressed BA bitmap with its size reduced significantly.

1.1.2.2 Legacy Protection, Coexistence, and Interoperability

With the introduction of multiple HT modes, co-existence of devices running at various modes can impose a major challenge in the deployment of 802.11n networks. On one hand, 802.11n devices have to co-exist with the 802.11 a/b/g devices in previously deployed wireless networks. For example, an inappropriately configured 802.11n device that runs in the Green Field mode can seriously affect the performance of a legacy 20 MHz device nearby since the latter is not able to recognize and yield to the GF signals properly. On the other hand, achieving interoperability is not trivial even among the 802.11n devices. There are quite a few 802.11n features that are optional. As a result, interoperability with other draft 802.11n devices is challenging. Compatibility with the future ratified standard can be another big concern.

L-SIG TXOP protection is one of the new protection mechanisms introduced in 802.11n to help the coexistence. As shown in Figure 1.8, in the L-SIG field of HT frames with a Mixed mode PHY header, the rate is always set to 6 Mbps and the length field can be set to some value that causes non-HT devices to defer transmission for a period of time. This effectively provides a protection mechanism for non-HT devices to defer transmission when a HT device is transmitting.

![Figure 1.8: Basic Concept of L-SIG Protection.](image)

To ensure the coexistence, it is required in 802.11n that GF mode operation must be protected when there are non-GF mode devices present nearby. It is also required that 40 MHz operation must be protected in the presence of non-HT devices.

1.2 IEEE 802.11k: Radio Resource Measurement

Emerging technologies and wireless applications (such as voice over IP, video over IP, location services, large scale WLAN deployment and management) impose many new requirements over the capabilities of WLANs. These advancements demand standardized facilities to acquire and exchange statistics and measurements to better deploy and manage the WLAN, to better utilize the wireless bandwidth, to automatically optimize network performance, and to improve the reliability of the WLAN. Such facilities are of key importance to the pre-eminence of 802.11 wireless networks.
Emerging IEEE 802.11 Standards

802.11k Radio Resource Measurement (RRM) specifies the facilities to meet the requirements of information about the radio environment. The specification defines Radio Resource Measurement enhancements by specifying a list of standardized measurements for radio resources and providing mechanisms to higher layers in the network stack for consistent radio and network measurement reports. The mechanisms include measurement requests and reports as well as the MIB with an Object Identifier (OID) interface to upper layers.

The provided radio measurements can be used for various benefits such as enabling simplified and automatic radio configuration, achieving better performance for the WLAN, optimizing the use of the client’s radio resources, alerting a network administrator to issues, notifying end user radio status, etc.

The 802.11k RRM measurements are exchanged with measurement pairs of requests and reports. The measurements include: Beacons, Measurement Pilots, summary of received packets, Noise Histograms, STA Statistics, Location Configuration Information, Neighbor Report, Link Measurements, QoS, QBSS Loads, Access Delay, etc.

802.11k adopts a layer management request/response model to collect statistics and perform measurements. In general, 802.11k only contains measurements that nearly all vendors can support via a driver or firmware upgrade without requiring hardware modifications.

1.3 802.11p: Wireless Access for the Vehicular Environment

IEEE 802.11p defines enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications, which includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). 802.11p is also referred to as Wireless Access for the Vehicular Environment (WAVE).

802.11p provides the lower layers of the Dedicated Short Range Communications (DSRC) solution and will be used as the groundwork for DSRC. DSRC is a U.S. Department of Transportation project. It targets at vehicle-based communication networks, especially for applications such as vehicle safety services, toll collections, and commerce transactions via cars. Its ultimate vision is a nationwide network that enables communications between vehicles and other vehicles or roadside access points. The higher layers of the DSRC solution are provided by standards outside of IEEE 802.11 family, such as IEEE 1609, IEEE 1556 for beacon authentication, and NEMO for mobility.

802.11p uses 5 and 10 MHz channels of 802.11 OFDM PHY at 5.9 GHz, with a spectral mask that cannot be easily met by 802.11a devices. It also requires a substantially extended MAC and uses only very few 802.11 facilities such as a basic access mechanism of EDCA.
1.4 802.11r: Fast BSS-Transitions

Prior to 802.11r, BSS transitions are supported under 802.11a/b/g, but only good enough for the best-effort data, not for QoS data. With the emergence of QoS applications, such as Voice over IP (VoIP), a satisfactory BSS transition solution for QoS data is required.

VoIP mobile phones are designed to work with wireless Internet networks. These VoIP devices must be able to disassociate from one access point and associate to another rapidly. The handoff delay typically cannot exceed a threshold of about 20 msec. There are several issues with the BSS transitions. For one thing, the handover latency is too long (often average in the hundreds of milliseconds) to support QoS traffic. This excess delay can lead to loss of call connectivity or degradation of voice quality. Another problem is that a VoIP device cannot know if necessary QoS resources are available at a new access point until after a transition. It is therefore impossible to know beforehand whether a transition will lead to satisfactory VoIP performance. In addition, it is also problematic for secure 802.11 connections using WPA2 or WPA.

802.11r defines enhancements to 802.11 required to provide a solution for fast BSS transition. It provides a faster handoff solution to address the needs of security, a minimal latency, and QoS resource reservation, which is essential to widely deployed VoIP applications. 802.11r will permit connectivity aboard vehicles in motion, with fast handoffs from one access point to another seamlessly.

802.11r allows a wireless client to establish a security and QoS state at a new access point before making a transition, which leads to minimal connectivity loss and application disruption. The overall changes of the roaming process do not introduce any new security vulnerabilities. This preserves the behavior of current stations and access points.

802.11r will govern the way roaming clients communicate with candidate APs for instance in establishing security associations and reserving QoS resources. Under 802.11r, clients can use the current AP as a passage to other APs, allowing clients to minimize disruptions caused by the roaming transition.

1.5 802.11s: Wireless Mesh Networks

802.11s defines enhancements to 802.11 required for a new topology of 802.11 wireless LANs, the Mesh Networks, which supports frame delivery in a hop-by-hop fashion. The work of 802.11s started in 2005 and its publication is expected by late 2008 or early 2009. Currently, the specification has been drafted and is in the stage of refinement.

802.11s inherits from existing 802.11 standards many features including security, QoS, and device power-saving mechanisms. For example, secure mesh links are set up based on 802.11i and push/pull key distribution using the key hierarchy and a mesh KDC, with fall back to pre-shared keys for small or home networks. It also adopts a variety of concepts such as Beacons and Probe/Response to advertise Mesh ID, Routing protocol, Security Capability etc.

802.11s defines a 6-address scheme to accommodate mesh tunneling. New mesh related features include route discovery, route maintenance, route recovery or re-establishment, and mesh routing functionality for frame routing and forwarding. In particular, 802.11s supports a layer 2 routing protocol for small and mid-size mesh
networks called hybrid wireless mesh protocol (HWMP), which is a hybrid of two wireless routing protocols: the Tree Based Routing and the AODV Routing. Both fixed and mobile mesh applications are supported by HWMP.

The major frame exchanges employed by HWMP include:

- PANN – portal announcement that enables mesh segmentation by allowing nodes to choose a portal as their gateway.
- RANN – root announcement that enables passive and active mesh formation (registration).
- RREQ – routing request that builds forward paths and enables registration of STAs at node
- RREP – routing response that builds reverse paths
- RRER – route error that signals the breaks-up of a path

1.6 802.11T: Wireless Performance Prediction

802.11T is developed to meet the need of the 802.11 industry for an objective means of evaluating functionality and performance of the increasingly sophisticated 802.11 products. Its goal is to define a set of testing methods and conditions and a set of performance metrics as a recommended practice to measure and predict performance in a consistent and uniform manner. These metrics are valuable to all involved in 802.11n products, including developers, end-users and product reviewers. 802.11T defines test metrics in the context of use cases, which are classified into three major groups: data, latency sensitive and streaming media.

The data applications include Web downloads, file transfers, file sharing, e-mails. Such traffic typically belongs to the best-effort access category in 802.11e. They do not put strict requirements on networks. The metrics important for data applications include throughput vs. range, AP capacity, and AP throughput per client.

Latency sensitive applications, such as voice over IP, are time-critical, whose traffic usually belong to the voice access category in 802.11e. Those applications impose a strict requirements of Quality of Service (QoS) over networks, including limits on voice latency, jitter and packet loss vs. range, network load, and admitted calls, etc.

Streaming-media applications include real-time audio/video streaming, stored content streaming, and multicast high-definition television streaming. These applications require even stricter QoS over networks than voice applications, including guarantees of bandwidth and latency. The related performance metrics include video quality (throughput, latency, jitter) vs. range and network load.

In addition to the above, there are other metrics such as throughput vs. path loss, fast BSS transition, receiver sensitivity, and AP capacity and association performance, etc.

The metrics are further classified as primary and secondary. The primary metrics (e.g., voice quality) directly affect the user experience. Secondary metrics, such as latency, jitter, and packet loss, affect the primary metrics and therefore indirectly affect the user experiences.

The recommended metrics are tested in the settings of either conducted (which provide RF isolation often in a shielded chamber and emulate controlled motion) or over-
the-air. For motion emulation and measurement repeatability, most of the tests require a conducted environment.

1.7 802.11u: Wireless Inter-working with External Networks

802.11u is an amendment to the 802.11 to add features that improve inter-working with external networks. 802.11u is still in its early stage of development. Its scope covers improved enrollment, network selection, emergency call support, user traffic segmentation, and service advertisement.

Current 802.11 assumes that a user is pre-authorized to use the network. 802.11u covers the cases where user is not pre-authorized. With 802.11u, a network will be able to allow access based on the user’s relationship with an external network (e.g., hotspot roaming agreements). A network can also indicate that online enrollment is possible or allow access to a strictly limited set of services such as emergency calls. This capability in 802.11u will also greatly improve the user experience of traveling users who will be able to select access to an external network based on the provided services and conditions for example.

There are a number of issues under considerations within IEEE 802.11 TGu, which include: wireless inter-working with external networks, requirements of address changes within the 802.11 PHY and MAC and enabling inter-working with non IEEE 802 networks.

802.11u has identified a set of mandatory requirements in the following clusters:

- Network Selection:
  - way to determine if a network in hotspot supports a particular SSPN (Subscription Service Provider Network) without authentication.
  - method for a client with multiple credentials to choose a proper one.
  - way for an AP to support multiple SSPNs.
  - method for a client to determine inter-working services before association.
- SSPN Interface: method to define the authorization information to be provided to the MAC and associated functionality.
- QoS Mapping: to define the mapping from external QoS information to 802.11 specific parameters.
- Media Independent Handover (MIH in 802.21).
- Emergency Sequence: to define the functionality for e911 call.

1.8 802.11v: Wireless Network Management

The existing mechanism in 802.11 for wireless network management is mostly via SNMP. However, there are quite a few issues for this approach. For example, not all wireless clients on the market possess SNMP capabilities. In the case that a wireless client cannot get IP connectivity, management of a device may be required, but use of SNMP is impossible then. In addition, the complexities of 802.11 APs nowadays require more